Express Mail EK830427695US DE920000036US1

Europäisches Patentamt | European Patent Office | Office européen des brevets

#4

Jc903 U.S. PTO 09/900637 07/06/01

Bescheinigung | Certificate | Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. | Patent application No. | Demande de brevet n°

00114612.5

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

I.L.C. HATTEN-HECKMAN

DEN HAAG, DEN
THE HAGUE, 22/01/01
LA HAYE, LE

Europäisches Patentamt
European Patent Office
Office européen des brevets

Blatt 2 der Bescheinigung
Sheet 2 of the certificate
Page 2 de l'attestation

Anmeldung Nr.:
Application no.: 00114612.5
Demande n°:

Anmeldetag:
Date of filing: 07/07/00
Date de dépôt:

Anmelder:
Applicant(s):
Demandeur(s):
International Business Machines Corporation
Armonk, NY 10504
UNITED STATES OF AMERICA

Bezeichnung der Erfindung:
Title of the invention:
Titre de l'invention:
System and method for secure comparison of a common secret of communicating devices

In Anspruch genommene Priorität(en) / Priority(ies) claimed / Priorité(s) revendiquée(s)

Staat:	Tag:	Aktenzeichen:
State:	Date:	File no.
Pays:	Date:	Numéro de dépôt:

Internationale Patentklassifikation:
International Patent classification:
Classification internationale des brevets:
/

Am Anmeldetag benannte Vertragstaaten:
Contracting states designated at date of filing: AT/BE/CH/CY/DE/DK/ES/FI/FR/GB/GR/IE/IT/LI/LU/MC/NL/PT/SE/TR
Etats contractants désignés lors du depôt:

Bemerkungen:
Remarks:
Remarques:

D E S C R I P T I O N

System and method for secure comparison of a common secret of communicating devices

Technical field

The present invention relates to system and method for secure comparison of a common secret of communicating devices, more particularly, to prove the authenticity of communicating devices within a client-server architecture using common secret shared by client and server.

Background or related prior art

Normally, authentication is required to work with remote server, to access data on a server, or to use a private network. The authentication can go in two directions. Either the server needs to prove its authenticity to the client, or the client needs to prove its authenticity to the server or both.

Therefore, either the server, or the client, or both must securely keep a private key. For the client key the portable smart card is ideal. It can securely store the private key and execute the required cryptographic algorithms with it.

The most important smartcard cryptographic protocols for authenticating devices are external and internal authentication.

External authentication means the authentication of an external device to the smartcard. The smartcard and the external device conduct a challenge-response protocol as follows:

1. The external device requests a random number from the smartcard by sending an appropriate command to the smartcard.

2. The smartcard creates a random number and returns it in the response to the external device.

3. The external device uses a cryptographic key corresponding to cryptographic key in the smartcard to encrypt the random number. It sends an authentication command containing the encrypted random number to the smartcard.

4. The smartcard receives the authentication command and decrypts the encrypted random number. If the result is equal to the stored random number, the smartcard assumes that the external device is authentic.

The cryptographic algorithms used for external authentication may be symmetric or asymmetric like DSA or RSA.

Internal authentication means the authentication of a smartcard to an external device. The smartcard and the external device conduct a communication protocol as follows:

1. The external device sends an authentication command containing a random number and the key number for specifying the key to be used by the smartcard.

2. The smartcard encrypts the random number received from the external device using the authentication key with the number specified in message of the external device and sends back the encrypted random number.

3. The external device decrypts the encrypted random number using the cryptographic key corresponding to the cryptographic key that has been used in the smartcard. If the result is equal the external device assumes that the smart card is authentic.

If a symmetric algorithm has been used, the external device and the smartcard must share a commona secret.

If a asymmetric algorithms is used, the external device uses a public key and the smartcard uses the corresponding private key.

Symmetric cryptographic algorithms are fast and can be used to encrypt and decrypt large amounts of data. However, the fact that the same key has to be used for encryption and decryption causes a problem when symmetric algorithms are to be used to ensure privacy of communication. The sender and receiver of a message must use the same key. Each receiver must know the keys of all potential senders to be able to decrypt all incoming messages.

The most famous asymmetric cryptographic algorithms are the public-key algorithms. Many public-key algorithms have been proposed, most of them insecure or impractical. The well known RSA algorithm for examples takes about 1000 times longer than DES, when implemented in hardware, 100 times longer.
Public-key algorithms use different keys for encryption and decryption. The private key may only be known to its owner and must be kept secret (smart card). It may be used for digital signature or for decrypting private information encrypted under the public key. The public key may be used for verifying digital signature or for encrypting information. It needs not to be kept secret because it is infeasible to compute the private key from a given public key.

Disadvantage of the prior art

Normally smartcards are ideal for storing secrets. However, a disadvantage of smartcards is their reduced storage capacity for storing cryptographic algorithms and digital keys, especially of storage-consuming algorithms like DES or RSA. Furthermore, storing keys into the smartcard in a secure way without allowing misuse of key and administer the keys by so-called trust centers requires an expensive and complicated infrastructure.
Finally, smartcards using cryptographic algorithms like DES or RSA are controlled by national export regulations.

It is therefore object of the present invention to provide a simplified and less storage consuming system and method for authentication between communicating devices having a common secret without exchanging the secret itself.

This object has been solved by the features of the independent claims. Further embodiments of the present invention are laid down in the subclaims.

Summary of the invention

The present invention relates to a simplified authentication system for communicating devices requiring less security requirements than conventional cryptographic systems.

The device to be authenticated includes at least a secret, a function component for generating a random number, a function component for exchanging messages with other devices and finally an algorithm for calculating a HASH using random number and secret. The device requesting authentication includes a secret and an algorithm for calculating a HASH using random number received from the device to to be authenticated. A function component for comparing both HASHs may be implemented in both systems. If the HASHs calculated by both devices matche it can be assumed that the authentication was successful.

This system and method may be used preferably within a commuication structure using portable communication devices like smartcards, personal digital assistants or mobile phones.

Neither an exchange of the plain secret itself nor the storage of digital keys is required. A misuse of the secret may be excluded by sending a HASH using random number and secret. The infrastructure required by the present invention is very simple and does not consume storage capacity like conventional encryption methods since digital keys and conventional symmetric or asymmetric algorithm are not required. Instead using the

digital keys and conventional symmetric - asymmetric algorithms, the present invention suggests to use a relatively simple random number and a simple HASH algorithm which sufficiently fulfills the security requirements of many communication architectures.

Brief Description of the Drawings

The present invention will be better understood and its numerous advantages will be come apparent to those skilled in the art by reference to the following drawings, in accordance with the accompanying specification, in which

FIG.1 is a generalized view of the components of the present invention

FIG.2 shows an implementation of the present invention in an e-commerce environment

FIG.3 shows an implementation of the present invention in a LAN-environment

FIG.4 shows the method of the present invention

FIG. 1 shows the basic components of the present invention. The present invention may be implemented in any communication architecture having at least a sender device 15 and a receiver device 10 communicating via wired or wireless network (e.g. LAN or Internet). A communication between sender 15 and receiver device 10 may be only established if an authentication protocol has been successfully executed. Sender device 15 which needs to be authenticated may be any portable or non-portable device either having a less storage capacity or do not require a conventional authentication system with a complex infrastructure. Receiver device 10 may be a any device offering services to the sender device 15 if the authentication succeeds. Preferably, receiver device 10 is a banking terminal, an automatic teller

machine or web server offering e-commerce application.

Sender device 15 (Device 2) includes a secret 56, which is identical with a secret 20 of the receiver device 65 and an algorithm 70 for calculating a HASH 80, which is identical with the HASH algorithm 30 of the receiver device 10. For example, the secret may be stored in a security module or a smart card belonging
to the sending device.

Sender's HASH algorithm 70 uses the secret 60 stored in the sender device 15 and identification data 56 generated by the sender device 10. Preferably, the secret 56 is a password or a PIN. Finally, sender device 15 includes a comparing component 90 comparing HASHs 80 of the sender 15 as well as the receiver device 40. In a preferred embodiment, sender's secret 56, sender's HASH algorithm 70 and comparing component 90 are stored in a smartcard. Access to the smartcard is made via a card reader which may be part of the sender device or a separate card reader connected with the sender device. Furthermore, sender device 15 includes a software component for generating identification data 55, e.g. random number. The identification data 55 is generated when executing an authentication protocol and is sent to the receiver device 10.

Receiver device 10 includes a secret 20 and an algorithm for calculating a HASH 30 (Device 1) using identification data 55 generated by the sender device 15 and PIN 20, 56 or password shared by sender and receiver device. For example, the secret may stored in a secure environment. Optionally, receiver 10 may also include a comparing component comparing the HASHs generated by sender 15 and receiver device 10 (not shown). In further embodiment, secret 20 of the receiver device 65, receiver HASH algorithm 30 and if available, comparing component may also be stored in a smartcard.

In a further embodiment, each communication device 15, 10 has

its own component for comparing the HASHs 90 as well as an own component for generating random numbers 55. This embodiment will be preferably used in a communication architecture in which both communication devices must be able to initiate an authentication process.

Assuming that the sender device 15 is card reader in which a smartcard is inserted and the receiver device 65 is an automatic teller machine, the method for accessing automatic-teller machine is as follows:

1. Terminal/card reader 15 initiates an authentication protocol sending Customer ID to the automatic-teller machine 10.
2. Automatic-teller machine 10 determines the associated PIN 20 to that customer using the customer ID.
3. Component 55 for generating a random number which is part of the card reader or smartcard 2 generates a random number and sends it to the automatic teller machine 10
4. HASH algorithm 30 of the automatic teller machine 10 and card reader/smartcard 15 generate a HASH 40, 80 using customer PIN 20, 56 and random number 55.
5. HASH 40 of the automatic-teller machine 10 is sent to the card reader/smartcard 15.
6. Component 90 for comparing the HASHs 90 which is part of the card reader/smart card 15 compares both HASHs. If the HASHs are equal access to the automatic-teller machine is allowed.

FIG. 2 shows an example of an e-commerce environment in which the present invention may be used.

The e-commerce provider offers e-commerce applications via a server 100. A potential customer may receive a password 110 from the e-commerce provider via a secure transmission way 120, e.g. by trusted delivery.

If the customer wants access to the e-commerce application he needs a password or PIN for accessing the e-commerce application. The plain password could be sent from the customer communication device (client-200) via Internet to the server 100 of the e-commerce provider however taking the risk that misuse of the password/PIN is possible. Avoiding such misuse conventional cryptographic algorithms are currently used with the consequence that an enormous cryptographic infrastructure is required.

That means in detail, digital keys in the size of 1024 and more bits and storage consuming cryptographic algorithms are required. Digital keys in that size are not perceptible by Customer.

Using the present invention, none digital keys as used by standard cryptographic systems are required but passwords or PINs having a small size of 8 bytes. Such passwords are easily perceptible by customer. The PIN or password does not leave the devices in its plain format. No key distribution (e.g. aymmetric cryptographic algorithms) is required. Furthermore, the HASH algorithm used by the present invention are simple and does not require a enormous cryptographic infrastructure like conventional prior art security systems requiring complex cryptographic algorithms. Preferably a secure HASH algorithm is used.

FIG. 3 shows an example of a LAN-environment in which the present invention may be used preferably. Shown is a typical client-server architecture. Client 40 and server 20 communicates via a insecure network 25. PIN 30 will be provided to the client 40, e.g. by a trusted delivery. The client 40 generates a random number and sends it to the server 20. On server 20 and client 40 side identical random number and identical PIN are provided to the HASH algorithm for generating a HASH. On the client side 40 a comparison of both HASHs is accomplished. If both HASHs are equal access to the server is

allowed.

Preferably, client's HASH algorithm and client's secret are stored in a security module of a smartcard. The smartcard is inserted in a card reader communicating with the server 20.

FIG. 4 shows inventive method in a client-server architecture as shown in FIG.3.

A server may receive a password or PIN from the server provider via a secure connection, e.g. by trusted delivery 10.
Client opens a session with the server, then generates a non-secret random number 20 and sends it to the server 30 via a insecure connection.

Client's HASH algorithm 40 and Server's HASH algorithm 90 calculate a HASH using common random number and common PIN.
Server sends the HASH calculated via the insecure connection to the client 50.

On the client side both HASHs will be compared 60.
If both HASHs are equal authentication is successful 70 and if both are unequal the authentication is failed 80.

C L A I M S

1. Method for authentication of communicating devices having a common secret, said method comprising the steps of:

receiving a HASH (40) by a receiving device (10) from a sending device (15)

comparing (90) said HASH (40) received from said sending device with a HASH (80) of said receiving device, wherein both HASHs are calculated by HASH algorithms using said identification data and said common secret.

2. Method according to claim 1, wherein said identification data (55) is generated by said sending device (15).

3. Method according to claim 2, wherein said identification data (55) is sent from said sending device (15) to said receiving device (10).

4. Method according to claim 1, wherein said HASHs algorithms are identical.

5. Method according to claim 1, wherein said common secret (20,56) may be a PIN or a password.

6. Method according to claim 1, wherein said identification data (55) is a random number.

7. Method according to claim 6, wherein said random number is generated by the operating system of said sending device or by a separat software component which is part of said sending device.

8. Method according to claim 1, wherein said comparing step may be accomplished by said sending or said receiving device.

9. Method according to claim 1, wherein said common secret (20, 56), said HASH algorithm (70) and said comparing component (90) of said sending device (15) are stored in a smartcard and communication between smartcard and receiving device is established via a card reader.

10. Method according to claim 9, wherein said smartcard and said card reader are part of a portable sending device.

11. Method according to claim 1, wherein the data connection between sending and receiving device is an insecure data connection.

12. Method according to claim 1, wherein said sending and said receiving device forms a client-server architecture.

13. Method according to claim 1, wherein said client is a portable device.

14. Client in a client-server architecture having an authentication system for executing the method according to claim to 1 to 13.

15. Server in a client-server architecture having an authentication system for executing the method according to claim 1 to 13.

16. Sender device communicating with a receiver device, wherein said sender or/and said receiver device comprising an authentication system for executing the

method according to claim 1 to 13.

17. Computer program product stored on a computer-readable media containing software code for performing of the method according to one of the claims 1 to 13 if the program product is executed on the computer.

A B S T R A C T

The present invention relates to a simplified authentication system for communicating devices requiring less security requirements than conventional cryptographic systems.

The device to be authenticated includes a secret, a function component for generating a random number, a function component for exchanging messages with other devices and finally an algorithm for calculating a HASH using random number and secret. The device requesting authentication includes a secret and an algorithm for calculating a HASH using random number received from the device to be authenticated. A function component for comparing both HASHs may be implemented in both devices. If the HASHs calculated by both devices match it can be assumed that the authentication was successful.
Preferably, this system and method may be used within a communication structure using portable communication devices like smartcards, personal digital assistants or mobile phones. Neither an exchange of the plain secret itself nor the storage of digital keys is required. A misuse of the secret may be excluded by sending a HASH using random number and secret. The infrastructure required by the present invention is very simple and does not consume storage capacity like conventional encryption methods since digital keys and conventional symmetric or asymmetric algorithms are not required. Instead of using the digital keys and conventional symmetric - asymmetric algorithms, the present invention suggests to use a relatively simple random number and a simple HASH algorithm, which sufficiently fulfills the security requirements of many communication architectures.

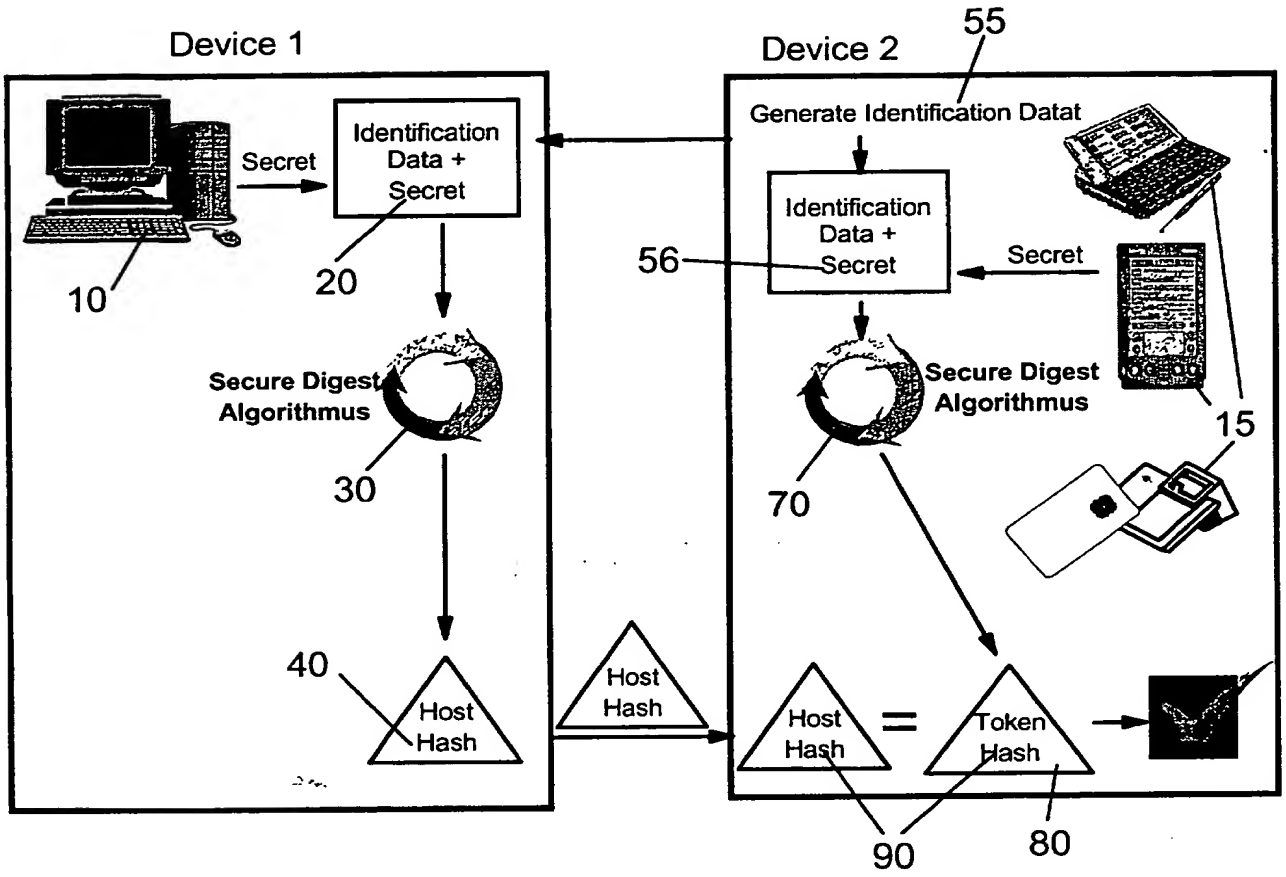
Device 1
Device 2
55
Generate Identification Datat
Identification Data + Secret
Secret
10
20
56
Secure Digest Algorithmus
30
70
15
40
Host Hash
Token Hash
90
80

FIG. 1

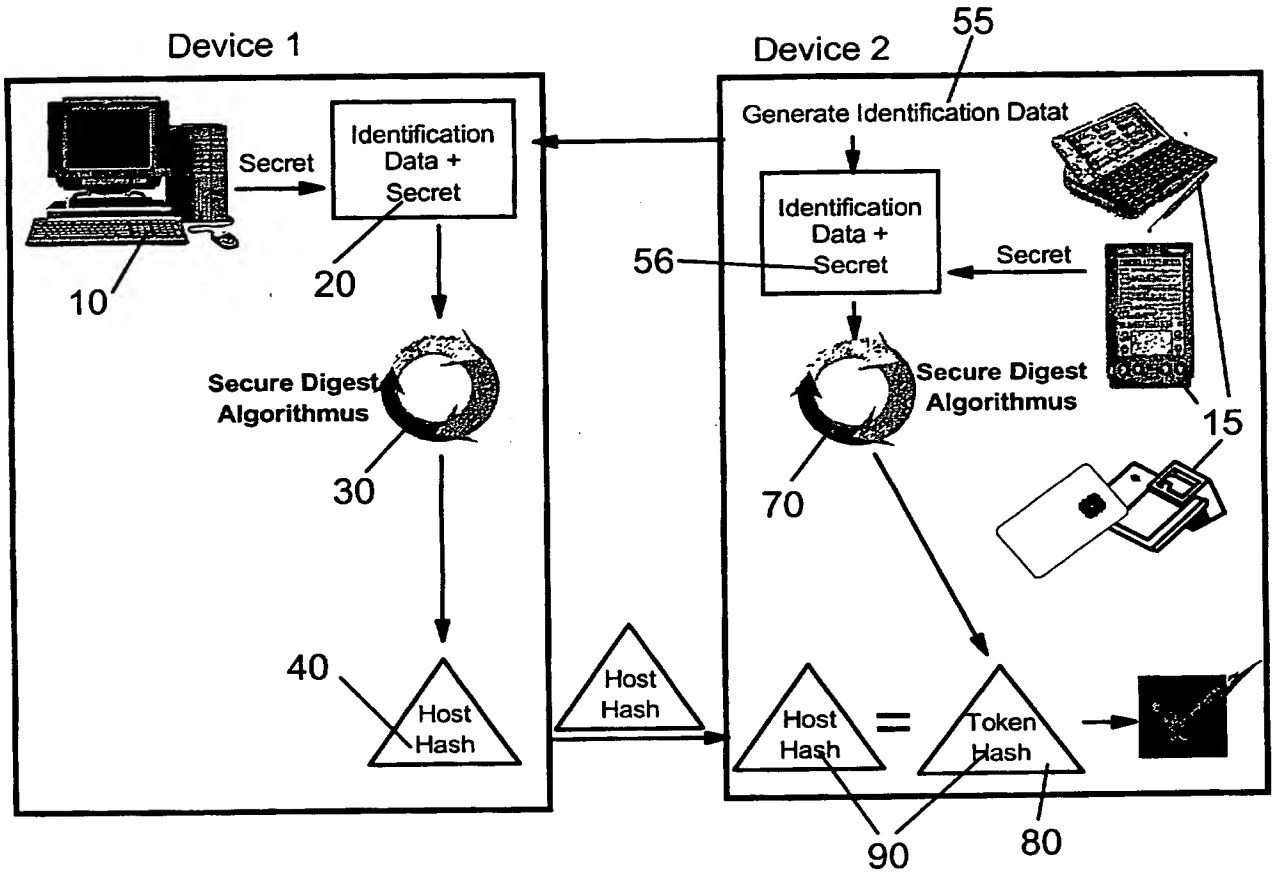

FIG. 1

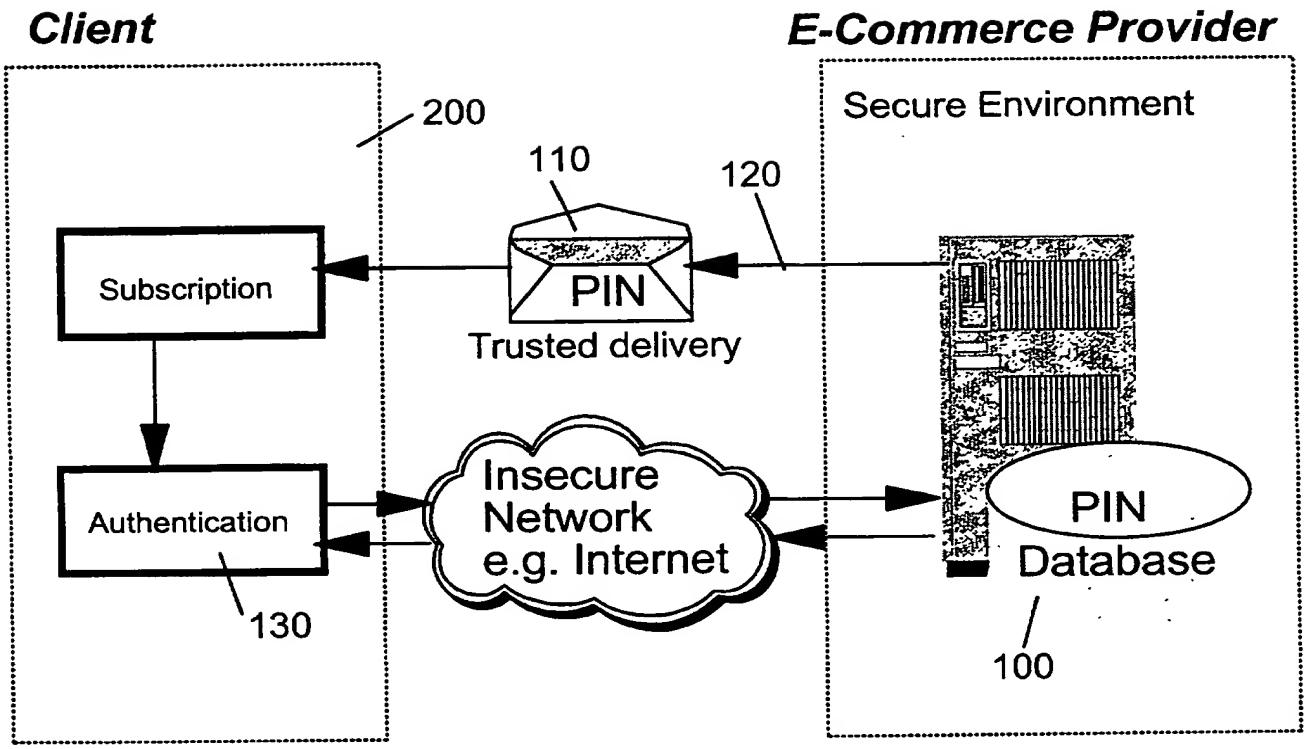
Client
E-Commerce Provider
Secure Environment
200
110
120
Subscription
PIN
Trusted delivery
Authentication
Insecure
Network
e.g. Internet
PIN
Database
130
100

FIG. 2

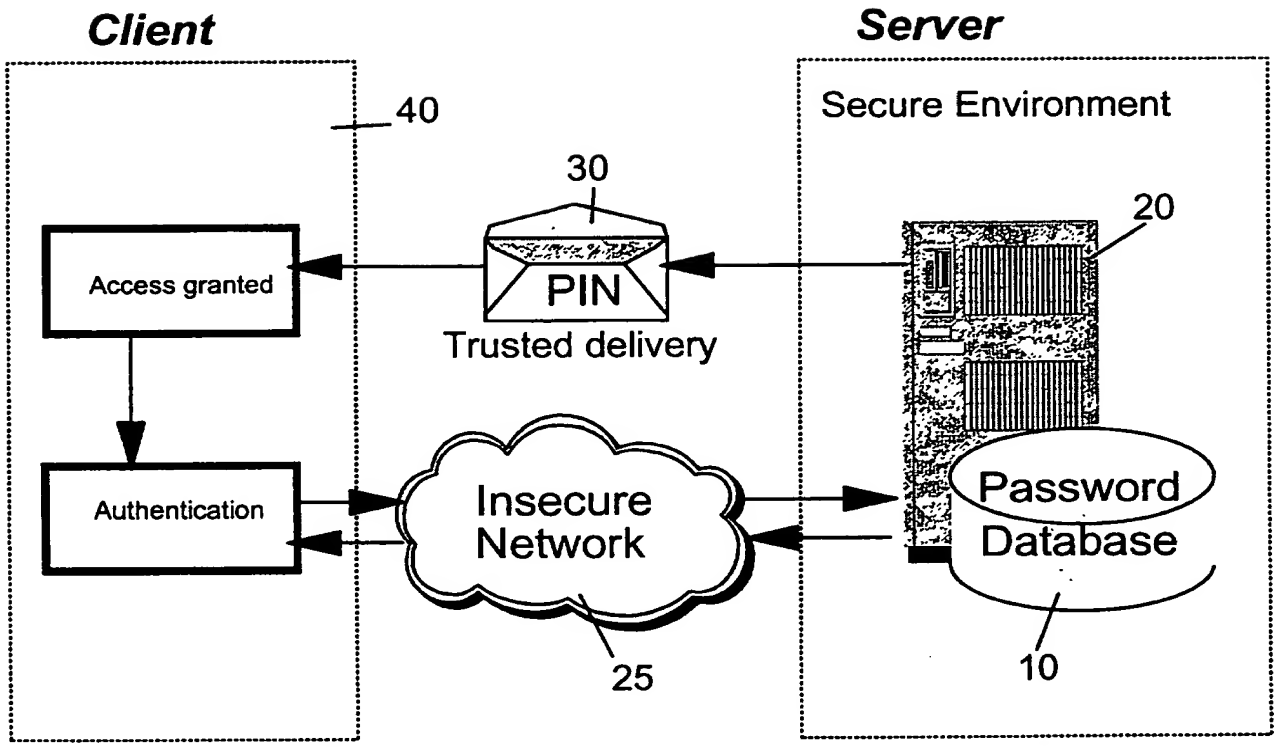
Client
Server
Secure Environment
40
30
20
Access granted
PIN
Trusted delivery
Authentication
Insecure
Network
Password
Database
25
10

FIG. 3

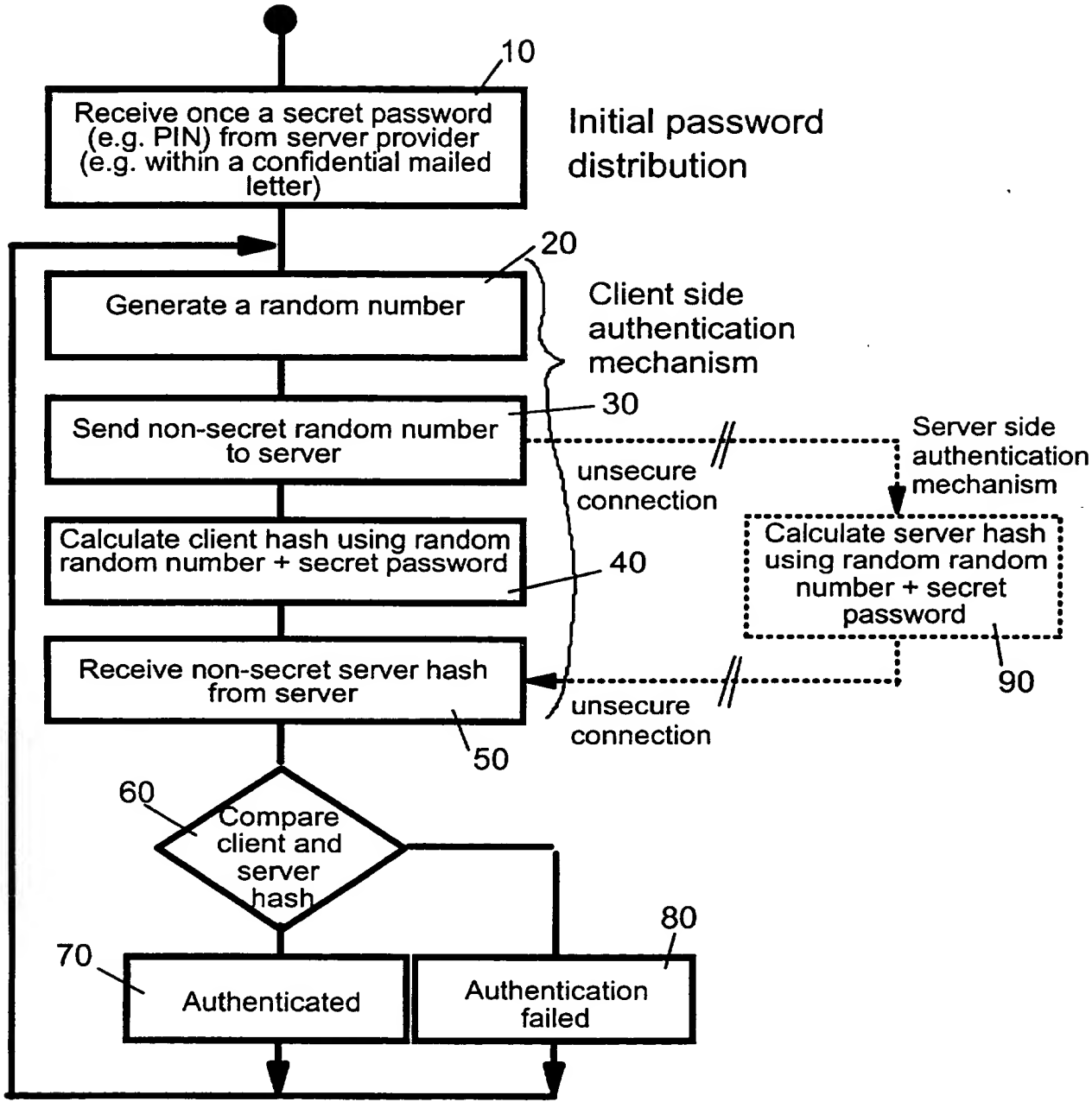
10
Receive once a secret password (e.g. PIN) from server provider (e.g. within a confidential mailed letter)
Initial password distribution
20
Generate a random number
Client side authentication mechanism
30
Send non-secret random number to server
unsecure connection
Server side authentication mechanism
Calculate client hash using random random number + secret password
40
Calculate server hash using random random number + secret password
90
Receive non-secret server hash from server
unsecure connection
50
60
Compare client and server hash
80
70
Authenticated
Authentication failed

FIG. 4